حمله ی Cross-site Scripting(XSS)

**تعریف و چرت و پرت های مربوط به XSS**

Bleach یک ماژول پایتون است که هر ورودی HTML را دریافت می کند و HTML معتبر و سالمی که فقط شامل زیرمجموعه مجاز برچسب ها(tags)، ویژگی ها (attributes ) و سبک (styles)های HTML است، را برمی گرداند. django-bleach یک برنامه جنگو است که استفاده از Bleach را بسیار آسان می کند.

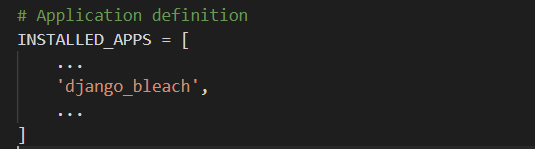
راه اندازی:

1. نصب

دریافت از گیت یا نصب با استفاده از Python Package Index مشابه زیر :

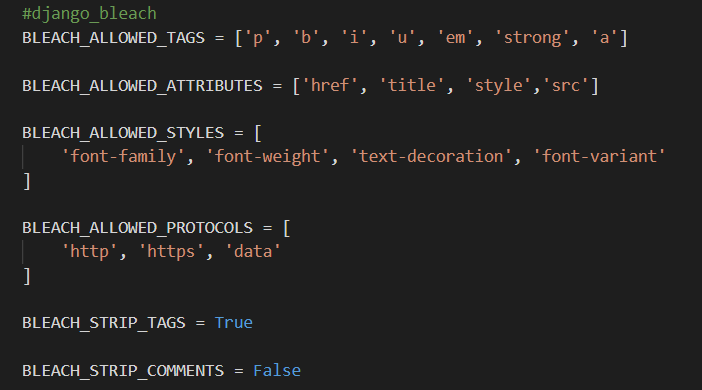
pip install django-bleach

1. اضافه کردن django\_bleach به مسیر settings.py



1. پیکربندی

django\_bleach با یک سری پیش فرض های معقول ارائه می شود اما با توجه به تنظیمات مورد نیاز ، آن ها را تغییر می دهیم.



3تنظیمات بالا به ترتیب به شرح زیر هستند:

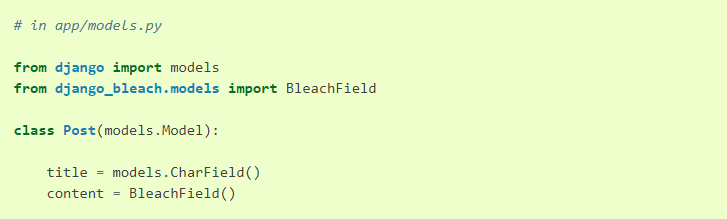
* تگ های مجاز HTML
* Attributeهای مجاز HTML
* ویژگی های مجاز CSS (با فرض اینکه style یک attribute مجاز است.)
* پروتکل ها و شبه پروتکل های مجاز (با فرض اینکه src یک attribute مجاز است.)
* حذف تگ های ناشناخته (در صورت True بودن)
* حذف commentهای HTML

1. استفاده و کاربرد

django\_bleach در سه مورد برای ایجاد خروجی bleachشده استفاده می شود:

* به کار بردن BleachFeild model feild

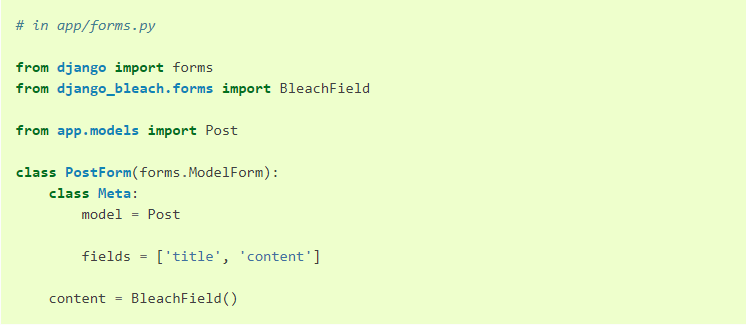
ساده ترین راه برای گنجاندن محتوای HTML قابل ویرایش توسط کاربر که به طور خودکار پاکسازی می شود، استفاده از فیلد BleachFeild model feild است. می توان آرگومان هایی نظیر allowed\_tags ، allowed\_attributes و ... که در setting برنامه تعریف شدند را برای دستیابی به اهداف خاصی به BleachFeild() اضافه کرد.



علاوه بر آرگومان‌های مخصوص ، فیلد مدل BleachField همه ویژگی‌های فیلد عادی را می‌پذیرد. در واقع در پشت صحنه، یک TextField است و همه آرگومان های مشابه TextField را می پذیرد.

* به کار بردن BleachFeild form field

این فیلد ورودی HTML کاربر را پاکسازی می‌کند و HTML ایمن و تمیز را به برنامه جنگو ارائه می‌کند و مقدار برگشتی "ایمن" علامت‌گذاری می‌شود.



فیلد فرم BleachField دقیقا همان آرگومان های فیلد مدل BleachField که در بالا توضیح داده شد را می گیرد.

* در صورت داشتن محتوایی که باید در یک template چاپ شود نیز از فیلتر bleach استفاده می کنیم.

